UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,757	01/15/2004	Bruce Moon	CISCP361/8157	6416

22434 7590 07/24/2006

BEYER WEAVER & THOMAS, LLP
P.O. BOX 70250
OAKLAND, CA 94612-0250

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 07/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/758,757	MOON ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/05 & 3/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to communication: original application filed on 15 January 2004.

2. Claims 1-21 are currently pending in this application. Claims 1, 12, 19, 20, and 21 are independent claims.

3. The IDS submitted August 2005 and March 2005 has been considered.

Drawings

4. The drawings are objected to because they contain multiple figures (i.e. 1, 2A, 2B, and 5) that are handwritten and contain sloppy text. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 1, 4, 6, 8-12, 15, 17, and 19-21,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahonen US Patent No. 6,976,177 (hereinafter '177).

As to independent claim 1, "A method of establishing a virtual private network tunnel, the method comprising: receiving, from a user whose IP address is not known in advance, a first request to form an encrypted tunnel with a security gateway" is taught in '177 col. 9, lines 6-35;

"forming the encrypted tunnel" is shown in '177 col. 9, lines 36-51;

"determining an IP address of the user; establishing a correspondence between the IP address and a first shared secret authorized for the user" is taught in '177 col. 10, lines 8-15;

"determining whether the first shared secret matches the second shared secret; and forming the virtual private network tunnel when the first shared secret matches the second shared secret" is shown in '177 col. 9 line 52 through col. 10, line 7 and col. 1, lines 43-47. the following is not explicitly taught in '177:

"authenticating the user" however '177 teaches "means for negotiating one or more Security Associations (SAs) between the mobile host and the Security Gateway (SG); (2) means

for subsequently initiating a communication between the mobile host and the SG using a negotiated SA and for receiving an authentication certificate sent from the mobile host, the certificate containing at least the identity of the mobile host and an IP address of the mobile host" and "the cryptographic identity of the mobile host 1; the (New) Source and Destination IP addresses (if changed); the ISAKMP Cookies of the mobile host 1 and the correspondent host 4, (under which the phase 2 negotiation was done); the IPsec protocol ID (AH, ESP); the SPI number of the phase 2 SA (usually the next available SA which was created during the preparations functions and which has not expired); current sequence number of the requested phase 2 SA (if this SA has been used earlier, then this number has increased in the counter of mobile host 1)" in col. 2, lines 62-67 and col. 9, lines 34-46, note the Security Association (SA) is known in the art to have the same meaning as authenticating the user.

"receiving a second request from the user to form a virtual private network tunnel, the request incorporating a second shared secret" however '177 teaches in col. 9, lines 43-46, note this update of a sequence depending upon the number of request has the same meaning as receiving a second request.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of establishing a Virtual Private Network (VPN) taught in '177 to include a means to allow a mobile client to request a second VPN. One of ordinary skill in the art would have been motivated to perform such a modification because of the increasing demand for mobility see '177 (col. 1, lines 11 et seq.) "There is an ever increasing demand for mobility in communications systems. However, this demand must be met in a manner which provides for the secure transfer of data between communicating parties. A concept known as the Virtual

Private Network (VPN) has recently been introduced, with the aim of satisfying, by a combination of encryption and secure access, this demand. A VPN may involve one or more corporate Local Area Networks (LANs) or intranets, as well as users coupled to "foreign" LANs, the Internet, wireless mobile networks, etc".

As to dependent claim 4, "wherein the second request comprises a request to form an IPSec tunnel" is taught in '177 col. 2, lines 5-10.

As to dependent claim 6, "wherein the second request incorporates a hashing function based on the second shared secret" is shown in '177 col. 2, lines 46-56.

As to dependent claim 8, "wherein the establishing step comprises making an entry in an IPSec table, the entry comprising the IP address and the first shared secret" is shown in '177 col. 8, lines 35-65 and col. 9, lines 51-57.

As to dependent claim 9, "wherein the entry is a temporary entry that is deleted after the occurrence of a predetermined event" is disclosed in '177 col. 2, lines 38-43.

As to dependent claim 10, "wherein the predetermined event comprises a passage of a predetermined time" is taught in '177 col. 2, lines 43-46.

As to dependent claim 11, "further comprising the step of tearing down the virtual private network tunnel when the temporary entry is deleted" is shown in '177 col. 10, line 66 through col. 11, line 6, and col. 12, lines 44-51.

As to independent claim 12, this claim is directed to the computer program comprising the instruction for a Security Gateway to implement the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 19, this claim is directed to a security gateway to implement the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 20, this claim is directed to a security gateway that incorporates the limitations of claim 1 plus the following limitations in bold that are also taught in '177:

"a first port configured for communication with the Internet" is shown in '177 col. 3, lines 57-60;

"a second port configured for communication with a private network" is disclosed in '177 col. 3, lines 57-67

"at least one processor configured to: receive, via the first port" is taught in '177 col. 3, lines 57-67.

As to independent claim 21, "A method of establishing a virtual private network tunnel, the method comprising: receiving, from a user whose IP address is not known in advance, a first request to form an encrypted tunnel with a security gateway" is taught in '177 col. 9, lines 6-35;

"forming the encrypted tunnel" is shown in '177 col. 9, lines 36-51;

"determining an IP address of the user; establishing a correspondence between the IP address and a subject of a digital certificate" is taught in '177 col. 10, lines 8-15 and col. 9, lines 20-34, (note a cryptographic certificate has the same meaning as a digital certificate, in addition applicant has acknowledged sending "digital certificates" when establishing a VPN as prior art see applicants publication US 2005/0160290 paragraph 0007);

"determining that the subject of the digital certificate is an expected subject; and forming the virtual private network tunnel when the first shared secret matches the second shared secret" is shown in '177 col. 9 line 52 through col. 10, line 7 and col. 1, lines 43-47, (note 'if the subject is expected' the 'Remote Control flag is set to "On", col. 10, line 1) the following is not explicitly taught in '177:

"authenticating the user" however '177 teaches "means for negotiating one or more Security Associations (SAs) between the mobile host and the Security Gateway (SG); (2) means for subsequently initiating a communication between the mobile host and the SG using a negotiated SA and for receiving an authentication certificate sent from the mobile host, the certificate containing at least the identity of the mobile host and an IP address of the mobile host" and "the cryptographic identity of the mobile host 1; the (New) Source and Destination IP addresses (if changed); the ISAKMP Cookies of the mobile host 1 and the correspondent host 4, (under which the phase 2 negotiation was done); the IPsec protocol ID (AH, ESP); the SPI number of the phase 2 SA (usually the next available SA which was created during the preparations functions and which has not expired); current sequence number of the requested phase 2 SA (if this SA has been used earlier, then this number has increased in the counter of mobile host 1)" in col. 2, lines 62-67 and col. 9, lines 34-46, note the Security Association (SA) is known in the art to have the same meaning as authenticating the user;

"receiving a second request from the user to form a virtual private network tunnel, the request incorporating the digital certificate" however '177 teaches in col. 9, lines 29-46 and , note this update of a sequence depending upon the number of request has the same meaning as receiving a second request.

As to dependent claims 15 and 17, these claim contain substantially similar subject matter as claims 4 and 6; therefore they are rejected along similar rationale.

7. **Claims 2, 3, 5, 13, 14, and 16,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '177 in view of Subramaniam et al. US Patent No. 6,640,302 (hereinafter '302).

As to dependent claim 2, the following is not taught in '177 **"wherein the first request comprises a request to form a Hypertext Transfer Protocol over Secure Socket Layer session"** however '302 teaches "The border server is connectable to the target server by a first communications link, such as an intranet or Ethernet link. The client is connectable to the border server by a second communications link, such as a TCP/IP link. The client and the border server are configured to support secure sockets layer communication over the second communications link using SSL or.similar software" in col. 3 lines 17-32.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of establishing a Virtual Private Network (VPN) taught in '177 to include a means to utilize SSL connections. One of ordinary skill in the art would have been motivated to perform such a modification because growth of secure networks see '302 (col. 1, lines 31 et seq.) "With the growth of such secure networks and their information content, there is an urgent need to support secure access by authorized users even when those users log in from a client machine outside the network security perimeter. A wide variety of tools and techniques relating to networks and/or security are known, at least individually and to at least some extent, including: computer network architectures including at least transport and session layers, sockets, clients, and servers; hyperlinks and uniform/universal resource locators (TVRLs); communications links such as Internet connections and LAN connections; proxy servers for

HTTP and some other protocols; internetworking; Kerberos authentication; authentication through certificates exchanged during an SSL handshake; tying certificates to access control lists so that users are identified in certificates presented during the SSL handshake instead of being identified by an IP address, DNS name, or username and password".

As to dependent claim 3, "wherein the authenticating step comprises receiving and verifying a username/password pair from the user" is taught in '302 col. 8, lines 45-62

As to dependent claim 5, "wherein the establishing step comprises comparing a username and password provided by the user with a database of usernames, passwords and shared secrets" is shown in '302 col. 9, lines 2-15 and '177 col. 9, lines 52-67.

As to dependent claims 13, 14, and 16, these claim contain substantially similar subject matter as claims 2, 3, and 5; therefore they are rejected along similar rationale.

8. **Claims 7 and 18,** are rejected under 35 U.S.C. 103(a) as being unpatentable over '177 in view of Jari et al. US Patent No. 6,907,532 (hereinafter '532).

As to dependent claim 7, the following is not explicitly taught in '177 **"wherein the step of determining whether the first shared secret matches the second shared secret comprises attempting to decrypt at least a portion of the second request"** however '532 teaches "The controller may be arranged to encrypt the security association database for storing in the non-volatile memory and to decrypt the security association database upon retrieval from the non-volatile memory" in col. 2, lines 33-36.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of establishing a Virtual Private Network (VPN) taught in '177 to include a means to decrypting communications. One of ordinary skill in the art would have been

motivated to perform such a modification to prevent unauthorized access see '532 (col. 1, lines 60 et seq.). "Security associations generally have a limited lifetime so as to prevent unauthorised access by deciphering each security association. When a security association reaches the end of its defined lifetime, it is replaced by another previously negotiated security association between the mobile user and the security gateway".

As to dependent claim 18, this claim contains substantially similar subject matter as claim 7; therefore it is rejected along similar rationale.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 8:30 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques H. Louis-Jacques can be reached on (571) 272-6962. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ECT

Ellen Tran
Patent Examiner
Technology Center 2134
18 July 2006

JACQUES LOUIS-JACQUES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100